(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 864 959 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
16.09.1998 Bulletin 1998/38

(51) Int. Cl.[6]: **G06F 1/00**

(21) Application number: **98104490.2**

(22) Date of filing: **12.03.1998**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **12.03.1997 JP 76555/97**

(71) Applicant:
MITSUBISHI CORPORATION
Chiyoda-ku Tokyo 100 (JP)

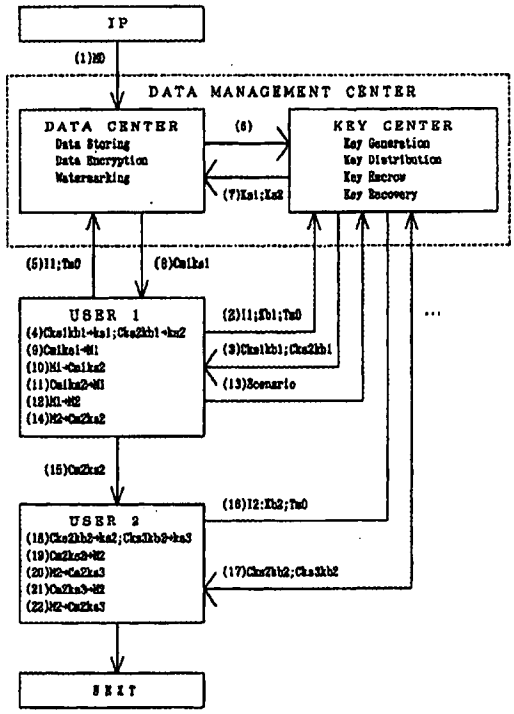
(72) Inventor: **Saito, Makoto**
Tama-shi (JP)

(74) Representative:
Neidl-Stippler & Partner
Rauchstrasse 2
81679 München (DE)

(54) Data management system

(57) To prevent piracy or leakage of data content, cryptography technique and electronic watermark technique are combined together and used. In a data content supplied to a user, a user data is entered as electronic watermark by a data management center, and the data content with electronic watermark entered in it is encrypted using a crypt key and is supplied. The encrypted data content is decrypted using a crypt key distributed from the data management center and is used. In case it is to be stored, it is encrypted using another crypt key. In case the data content is copied and transferred to another user, a user data of said another user is entered as electronic watermark, and a scenario to enter the user data of said another user as electronic watermark is registered at the data management center, and the data content with electronic watermark entered in it is encrypted using another crypt key and is supplied. When the validity of said another user is confirmed by the scenario, another crypt key is distributed to said another user. The encrypted data content is decrypted using another crypt key and is used. When it is to be stored, it is encrypted using a still another key. In case the data content has been copied and transferred illegitimately, it is possible by verifying the electronic watermark to identify the user who has copied and transferred the data content illegitimately.

Fig. 1



EP 0 864 959 A2

Printed by Xerox (UK) Business Services
2.16.3/3.4

Description

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to a system for managing data for using, i.e., storing, copying, editing, or transferring digital data content.

BACKGROUND ART

Because analog data content is deteriorated in quality whenever storing, copying, editing, or transferring it, controlling copyrights associated with these operations has not been a serious problem. However, because digital data content is not deteriorated in quality after repeatedly storing, copying, editing, or transferring it, such controlling copyrights associated with these operation is a serious problem.

Because there has been hitherto no adequate method for controlling a copyright for digital data content, the copyright is handled by the copyright law or contracts. Even in the copyright law, compensation money for a digital-type sound- or picture-recorder is only systematized.

Use of a data content includes not only referring to its contents but also normally effectively using by storing, copying, or editing obtained data content. Moreover, it is possible to transmit edited data content to another person via on-line basis by a communication line or via off-line basis using a proper recording medium. Furthermore, it is possible to transmit the edited data content to the database to be registered as new data content.

In a conventional database system, only character data content is handled. In a multimedia system, however, audio data content and picture data content which are originally analog data contents are digitized and formed into a database in addition to the data content such as characters which have been formed into a database so far.

Under these circumstances, how to deal with a copyright of data content in a database is a large problem. However, there has not been adequate copyright management means for solving the problem so far, particularly copyright management means completed for secondary utilization such as copying, editing, or transferring of the data content.

The inventor of the present invention proposed a system for managing a copyright by obtaining a permit key from a key control center via a public telephone line in Japanese Patent Laid-Open No. 46419/1994 (GB2269302A) and Japanese Patent Laid-Open No. 141004/1994 (USP5,504,933) and moreover, proposed an apparatus for managing the copyright in Japanese Patent Laid-Open No. 132916/1994 (GB2272822A).

Moreover, a copyright management method for primary utilization of digital data content such as display (including process to sound) or storage including real-time transmission of the digital data content in a database system and secondary utilization of the digital data content such as copying, editing, or transferring of the digital data content by further developing the above invention is proposed in Japanese Patent Application No. 64889/1994 (USSN08/416,037).

The database copyright management system of the above application in order to manage the copyright, either one or more of a program for managing the copyright, copyright information, and a copyright control message are used in addition to a use permit key corresponding to a requested use, and data content which has been transferred with encrypted is decrypted to be used for viewing and editing, and the data content is encrypted again when used for storing, copying and transferring.

The copyright control message is displayed, when utilization beyond the range of the user's request or authorized operation is found, to give caution or warning to a user and the copyright management program performs monitoring and managing so that utilization beyond the range of the user's request or authorized operation is not performed.

On the other hand, it is widely practiced to establish LAN (Local Area Network) by connecting computers with each other in offices, organizations, companies, etc. Also, a plurality of networks are connected with each other, and Internet is now organized in global scale, by which a plurality of networks are utilized as if these are a single network.

In LAN used in an organization such as firms, secret information is often stored, which must not be disclosed to outsiders.

For this reason, it is necessary to arrange the secret information in such manner that only a specific group of users can gain access and use such information, and such access is generally placed under control to prevent leakage of secret information to outsiders.

There are roughly two methods to control the access: a method to control access with access permission, and a method to do it by encryption.

The method of access control by access permission is described in U.S. Patents 5,173,939, 5,220,604, 5,224,163, 5,315,657, 5,414,772 and 5,438,508, in EP506435, and in JP Laid-Open 169540/1987.

The access control method based on encryption is disclosed in U.S. Patents 4,736,422, 5,224,163, 5,400,403, 5,457,746, and 5,584,023, in EP438154 and EP506435, and in JP Laid-Open 145923/1993. The access control

method based on encryption and digital signature is described in U.S. Patents 4,919,545 and 5,465,299.

Intranet is now being propagated, in which a plurality of LANs are connected with each other via Internet and these LANs are utilized as if they are a single LAN.

In this Intranet, information exchange is performed via Internet, which basically provides no guarantee for prevention of piracy, and information is encrypted to prevent the piracy when secret information is exchanged.

The prevention of information piracy during transmission by means of encryption is disclosed in U.S. Patents 5,504,818 and 5,515,441, and the use of a plurality of crypt keys is described in U.S. Patents 5,504,816, 5,353,351, 5,475,757, and 5,381,480. Also, performing re-encryption is described in U.S. Patent 5,479,514.

When encrypting, management of crypt key including transfer and receipt of crypt key becomes an important issue. Generation of keys by IC card is disclosed in U.S. Patent 5,577,121, and encryption/decryption by IC card is disclosed in U.S. Patents 5,347,581 and 5,504,817.

Also, electronic watermark technique is discribed in EP649074.

In the video conference system, a television picture has been added to the conventional voice telephone set. Recently the video conference system is advanced in which a computer system is incorporated in the video conference system so that the quality of the voice and the picture are improved, and data content can be handled at the same time as well as the voice and the picture.

Under these circumstances, security against the violation of the user's privacy and the data content leakage due to eavesdropping by persons other than the participants of the conference are protected by the cryptosystem using a secret-key.

However, since the conference content obtained by the participants themselves are decrypted, in the case where participants themselves store the content of the conference and sometimes edit the content, and further, use for secondary usage such as distribution to the persons other than the participants of the conference, the privacy of other participants of the video conference and data content security remains unprotected.

In particular, the compression technology of the transfer of data content is advanced while the volume of the data content storage medium is advanced with the result that the possibility is getting more and more realistic that all the content of the video conference may be copied to the data content storage medium or transmitted via a network.

Also, electronic commerce system with digital data content for commercial dealing is now being used for practical application. Above all, various types of experiments are now under way for digital cash system to exchange electronic data content instead of cash so that the system can be used by general public.

The digital cash system which has been proposed so far is based on a secret-key cryptosystem. The encrypted digital cash data content is transferred from a bank account or a cash service of a credit company, and is stored in an IC card so that a terminal device for input/output is used to make a payment. The digital cash system which uses this IC card as a cash-box can be used at any place such as shops or the like as long as the input/output terminal is installed. However, the system cannot be used at places such as homes or the like where no input/output terminal is installed.

Since the digital cash is an encrypted data content, any device can be used as the cash-box which stores digital cash data content, in addition to the IC card, as long as the device can store encrypted data content and transmit the data content to the party to which the payment is made. As a terminal which can be specifically used as the cash-box, there are personal computers, intelligent television sets, portable telephone sets such as personal digital assistant (PDA), personal handyphone system (PHS), intelligent telephone sets, and PC cards or the like which has an input/output function.

It is desirable that the digital cash is processed as an object associated with data content and functions instead of being as a simple data content.

In handling a digital cash, there are a common digital cash form, an unentered digital cash form private for an owner, an entry column in the digital cash form private for the owner, a digital cash data content showing an amount of money, an instruction of handling digital cash, and a digital cash form private for the owner in which an amount of money is entered. In an object-oriented programming, concepts such as an object, a class, a slot, a message and an instance are used.

In these correspondence relations, the common digital cash form is the object; the unentered digital cash form private for an owner: the class; the entry column of a digital cash form private for the owner: the slot; the instruction of handling digital cash: the message; and the digital cash form private for the owner in which an amount of money is entered: the instance.

A digital cash data content comprising the amount of money and the like is used as an argument, then, is transferred and stored in the slot which is referred to as an instance variable by the message so that a new instance is made which is a digital cash in which the amount of money is renewed.

The encryption technique used in the data management system is utilized not only in the distribution of copyrighted data content but also in the distribution of digital cash.

Then, basic encryption-related technique used in the present invention will be described below.

--Crypt key--

Secret-key system is also called "common key system" because the same key is used for encryption and decryption, and because it is necessary to keep the key in secret, it is also called "secret-key system". Typical examples of encryption algorithm using secret- key are: DES (Data Encryption Standard) system of National Bureau of Standards, FEAL (Fast Encryption Algorithm) system of NTT, and MISTY system of Mitsubishi Electric Corp. In the embodiments described below, the secret- key is referred as "Ks".

In contrast, the public-key system is a cryptosystem using a public-key being made public and a private-key, which is maintained in secret to those other than the owner of the key. One key is used for encryption and the other key is used for decryption. Typical example is RSA public-key system. In the embodiments described below, the puBlic-key is referred as "Kb", and the priVate-key is referred as "Kv".

Here, the operation to encrypt data content, a plain text material M to a cryptogram Cks using a secret-key Ks is expressed as:

$$Cks = E(M, Ks).$$

The operation to decrypt the cryptogram Cks to the plain text data content M using a secret-key Ks is expressed as:

$$M = ID(Cks, Ks).$$

Also, the operation to encrypt the plain text data content M to a cryptogram Ckb using a public-key Kb is expressed as:

$$Ckb = E(M, Kb).$$

The operation to decrypt the cryptogram Ckb to the plain text data content M using a private-key Kv is expressed as:

$$M = D(Ckb, Kv).$$

The operation to encrypt the plain text data content M to a cryptogram Ckv using a private-key Kv is expressed as:

$$Ckv = E(M, Kv),$$

and the operation to decrypt the cryptogram Ckv to the plain text data content M using the public-key Kb is expressed as:

$$M = D(Ckv, Kb).$$

The encryption technique is the means to exclude illegitimate use of data content, but perfect operation is not guaranteed. Thus, the possibility of illegitimate use of data content cannot be completely excluded.

On the other hand, electronic watermark technique cannot exclude the possibility of illegitimate use, but if illegitimate use is detected, it is possible to check the illegitimate use by verifying the content of electronic watermark, and there are a number of methods in this technique. These methods are described in Nikkei Electronics, No.683, 2-24-1997, pp.99-124, "'Digital watermark' to help stop to use illegal proprietary digital works in the multimedia age". Also, description is given on this technique by Walter Bender et al.: "Introducing data-hiding technology to support digital watermark for protecting copyrights" (IBM System Journal, vol. 35, Nos. 3 & 4, International Business Machines Corporation).

SUMMARY OF THE INVENTION

To prevent piracy or leakage of data content, cryptography technique and electronic watermark technique are combined together and used.

In a data content supplied to a first user, a first user data is entered as electronic watermark by a data management center, and the data content with electronic watermark entered in it is encrypted using a crypt key and is supplied. The encrypted data content is decrypted using a crypt key distributed from the data management center and is used. In case it is to be stored, it is encrypted using another crypt key.

In case the data content is copied and transferred to a second user, a user data of the second user is entered as electronic watermark, and a scenario to enter the user data of the second user as electronic watermark is registered at the data management center, and the data content with electronic watermark entered in it is encrypted using another

crypt key and is supplied. When the validity of the second user is confirmed by the scenario, another crypt key is distributed to the second user. The encrypted data content is decrypted using another crypt key and is used. When it is to be stored, it is encrypted using a still another key.

In the data content obtained by the first user, the first user data is entered as electronic watermark by a data center. If the data content is copied and transferred without taking normal procedure, the data center verifies the electronic watermark entered therein, and it is possible to detect the first user who has copied and transferred the data content without taking normal procedure.

When it is copied and transferred by normal procedure, electronic watermark of each user is entered, and this makes it possible to clearly define the route of copying and transfer. When copying and transfer are repeated, noise in the data content is increased by the entered electronic watermark, and this makes it possible to limit copying and transfer usage which may increase the risk of illegitimate utilization of data content.

Because a key used for encryption of the data content is stored at the key center, the key center can be utilized when a key escrow system or a key recovery system is used in practical application.

Further, the secret-key can be used as user data and the secret-key is encrypted using the public-key of the data center and this is entered as electronic watermark. By decrypting this using the private-key of the data center when necessary and by confirming the secret-key, it is possible to achieve a key escrow system or a key recovery system in simple manner but with high security.

In addition to copyright management of data content using a charged crypt key, the present invention is also applicable in the applications such as maintenance of privacy of participants in a video conference based on a video conference system using a free-of-charge crypt key and also for maintenance of security of the data content, or the maintenance of data security in electronic data interchange (EDI) such as electronic commerce.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a data management system of a first embodiment of the present invention;
Fig. 2 is a block diagram of a data management system of a second embodiment of the present invention;
Fig. 3 is a block diagram of a data management system of a third embodiment of the present invention;
Fig. 4A and Fig. 4B each represents a flow chart of processing in the data management system of a fourth embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[Embodiment 1]

Description will be given now on the first embodiment of the invention referring to Fig. 1.

(1) A data management center comprises a data center and a key center, while these may be organizations independent from each other.

At the data center in the data management center, data content M0 of IP (information provider) may be stored in database in advance or may be transferred from IP each time at the request of a first user U1.

(2) The first user U1 specifies a data content name Tm0 to the key center, presents a user data I1 and a public-key Kb1 of the first user, and requests the distribution of a secret-key Ks1 for decryption and a secret-key Ks2 for re-encryption.

As the user data, a user ID, a user E-mail address or a secret-key generated at the user's request for secret-key can be used. Further, random number prepared by the data center as the one specific for the user can be used.

Also, it may be designed in such manner that the data management center combines the first user information (having data amount of several tens of bytes in general) with the first user public-key Kb1 (having data amount of about 1000 bits) and obtains a first user data I1 (having data amount of one thousand and several hundreds of bits), and that MD5 hash value of 16 bytes, obtained by turning the first user data I1 to bash value by MD5 hash algorithm, can be used as the user data.

(3) The key center generates the secret-keys Ks1 and Ks2 and stores them together with the data content name Tm0, the first user data I1 and the first user public-key Kb1, and the secret-keys Ks1 and Ks2 are encrypted using the first user public-key Kb1:

$$Cks1kb1 = E(Ks1, Kb1)$$

$$Cks2kb1 = E (Ks2, Kb1)$$

and the encrypted secret-keys Cks1kb1 and Cks2kb1 are distributed to the first user.

(4) The first user U1 decrypts the distributed encrypted secret-keys Cks1kb1 and Cks2kb1 using the first user private-key Kv1:

$$Ks1 = D (Cks1kb1, Kv1)$$

$$Ks2 = D (Cks2kb1, Kv1).$$

The decrypted secret-keys Ks1 and Ks2 are stored in the device. The user is not the owner of the secret- keys Ks1 and ks2, but the key center or the data center is the owner. Because there may be possibility of improper use of the secret-keys if the management of the secret-keys is made by the user, the secret- keys Ks1 and Ks2 are automatically stored in IC card, PCMCIA card, insert board or software which are not under user's control.

Here, the fee to use the data content M0 is charged.

The secret-keys Ks1 and Ks2 can be generated using the first user data I1. If the data content name and the first user data I1 are available, Ks1 can be generated again. Therefore, it will suffice that the data content name Tm0, the first user data I1 and the first user public-key Kb1 are stored.

The secret-keys may be selected each time from library of the key center instead of generating them.

Japanese Patent Laid-Open 271865/1995, as filed by the present inventor, describes a method to divide a copyright management program and to distribute by attaching to each data content and key.

This method can be applied to the secret-keys themselves, and the secret-key Ks1 can be divided to partial secret-keys Ks11 and Ks12 as:

$$Ks11 + Ks12 = Ks1$$

and the secret-key Ks2 can be divided to partial secret-keys Ks21 and Ks22 as:

$$Ks21 + Ks22 = Ks2.$$

The partial secret-keys Ks11 and Ks21 are distributed as partial secret-keys, and the remaining partial secret-keys Ks12 and Ks22 are attached to the data content and distributed. Then, the first user cannot engage any more in the management of the secret-keys Ks1 and Ks2.

(5) The first user U1 presents the first user data I1, specifies the data content name Tm0; and requests the distribution of the data content M0 to the data center.

(6) The data center transfers the first user data I1 and the data content name Tm0 presented by the first user to the key center and asks to transfer the secret-keys Ks1 and Ks2.

(7) The key center transfers the secret-keys Ks1 and Ks2 to the data center.

(8) The data center encrypts the first user data I1 using the public-key Kb0 of the data center:

$$Ci1kb0 = E (I1, Kb0),$$

and the encrypted first user data Ci1kb0 is entered as an electronic watermark Wci1kb0 to the data content M0 requested by the first user U1, and a data content M1 with electronic watermark is edited as:

$$M1 = M0 + Wci1kb0.$$

And this is further encrypted using the secret-key Ks1:

$$Cm1ks1 = E (M1, Ks1),$$

to be an encrypted electronic watermaked data content Cm1ks1. This is distributed to the first user U1 by data com-

munication or data broadcasting or by recording on a medium.

The scenario of editing process of the data content M1 (information relating to electronic watermark such as the first user data) is stored to be used for verification.

As a simplified procedure, the first user data I1 may be entered as an electronic watermark Wi1 instead of the encrypted first user data Cilkb0 for the electronic watermark.

(9) The first user U1 decrypts the encrypted electronic watermarked data content Cm1ks1 using the secret-key Ks1 for decryption:

$$M1 = D (Cm1ks1, Ks1)$$

and uses it.

In this case, the secret-key Ks1 is abandoned by the procedure such as overwriting of the secret-key Ks2 on the secret-key Ks1.

(10) When the data content M1 is stored in the storage unit, the data content M1 is re-encrypted using the secret-key Ks2 for re-encryption:

$$Cm1ks2 = E (M1, Ks2)$$

and it is stored as a re-encrypted data content Cm1ks2.

(11) When the first user re-uses the re-encrypted data content Cm1ks2, the first user U1 reads the re-encrypted data content Cm1ks2 stored in the storage unit on memory, and decrypts it using the secret-key Ks2 and uses it. When the first user stores the data content M1 again, the data content M1 is re-encrypted using the secret-key Ks2 for re-encryption, and the re-encrypted data content Cm1ks2 is stored in the storage unit.

(12) In case the first user transfers the data content M1 to a second user U2, the first user U1 encrypts a second user data I2 using a public-key Kb0 of the data center:

$$Ci2kb0 = E (I2, Kb0),$$

enters the encrypted second user data Ci2kb0 as electronic watermark Wci2kb0 to the data content M1 requested by the second user U2 and edits to a data content M2 with electronic watermark:

$$M2 = M1 + Wci2kb0 = (M0 + Wci1kb0) + Wci2kb0.$$

As a simplified procedure, the second user data I2 may be entered as electronic watermark Wi2 instead of the encrypted second user data Ci2kb0.

(13) After the data content M1 with electronic watermark is edited to the data content M2 with electronic watermark, the first user U1 transfers the scenario of editing process of the edited data content M2, i.e., information relating to electronic watermark such as the second user data, to the key center and registers it. As a result, the second user can use the data content.

(14) Further, the first user U1 encrypts the data content M2 with electronic watermark using the secret-key Ks2:

$$Cm2ks2 = E (M2, Ks2)$$

and encrypted electronic watermarked data content Cm2ks2 is obtained.

(15) The first user U1 transfers the encrypted electronic watermarked data content Cm2ks2 to the second user U2 by data communication or by copying it on a medium.

(16) The second user U2 stores the transferred encrypted electronic watermarked data content Cm2ks2 in the storage unit.

The second user U2 specifies the data content name Tm0 to the key center, presents a public-key Kb2 of the

second user, and requests the distribution of the secret-key Ks2 for decryption and a secret-key Ks3 for re-encryption.

(17) The key center confirms according to the stored scenario that the second user U2 is a valid user and generates the secret-key Ks3 and stores it. Then, the stored secret-key Ks2 and the generated secret-key Ks3 are encrypted using the public-key Kb2 of the second user:

$$Cks2kb2 = E (Ks2, Kb2)$$

$$Cks3kb2 = E (Ks3, Kb2).$$

Then, the encrypted secret-key Cks2kb2 and the encrypted secret-key Cks3kb2 are distributed to the second user U2.

(18) The second user U2 decrypts the encrypted secret-keys Cks2kb2 and Cks3kb2 using a private-key Kv2 of the second user:

$$Ks2 = D (Cks2kb2, Kv2)$$

$$Ks3 = D (Cks3kb2, Kv2).$$

The decrypted secret-keys Ks2 and Ks3 are stored in IC card, PCMCIA card, insert board or software.

The secret-keys Ks2 and Ks3 at the second user are handled and are decrypted and stored in the same manner as the secret-keys Ks1 and Ks2 at the first user.

(19) The second user U2 reads the encrypted electronic watermarked data content Cm2ks2 stored in the storage unit on memory and decrypts it using the stored secret-key Ks2:

$$M2 = D (Cm2ks2, Ks2)$$

and uses it.

In this case, the secret-key Ks2 is abandoned by the procedure such as overwriting of the secret-key Ks3 on the secret-key Ks2.

(20) When the data content M2 is stored again in the storage unit, the data content M2 is re-encrypted using the secret-key Ks3 for re-encryption and is stored as the re-encrypted data content Cm2ks3.

(21) When the second user U2 re-uses the re-encrypted data content Cm2ks3, the re-encrypted data content Cm2ks3 stored in the storage unit is read on memory, and it is decrypted using the secret-key Ks3 and is used.

(22) When the second user stores the data content M2 again, the data content M2 is re-encrypted using the secret-key Ks3 for re-encryption, and the re-encrypted data content Cm2ks3 is stored in the storage unit.

Then, the same procedure is repeated.

The embodiment as described above is arranged under the assumption that the transferred data content is utilized at real time, while it may be designed in such manner that the data content obtained in advance and stored by the user is decrypted later and is used.

In such case, the first user is at the position of the second user in the above embodiment, and similar operation is performed.

As it is evident from the above description, the first user data is entered as electronic watermark in the data content obtained by the first user by the data center.

Therefore, if it is copied and transferred without taking normal procedure, the data center verifies the electronic watermark entered therein, and it is detected that the first user has copied and transferred it without taking normal procedure.

When it is copied and transferred by normal procedure, electronic watermark of each user is entered in the data content, and this clears the route of copying and transfer. When copying and transfer are repeated, noise in the data content increases by the entered electronic watermark, and this makes it possible to limit copying and transfer usage which may increase the risk of illegitimate utilization.

Because a key used for encrypting the data content is stored at the key center, the key center can be utilized when a key escrow system or a key recovery system is used in practical application.

Further, the secret-key can be used as user data, and the secret-key is encrypted using the public-key of the data center and this is entered as electronic watermark. By decrypting this using the private-key of the data center when necessary and by confirming the secret-key, it is possible to achieve a key escrow system or a key recovery system in simple manner but with high security.

[Embodiment 2]

Description will be given now on a second embodiment of the invention referring to Fig. 2.

(1) A data management center comprises a data center and a key center, while these may be organizations independent from each other.

At the data center in the data management center, a data content M0 of IP (information provider) is stored in database in advance or the data content M0 is transferred from IP each time at the request of the first user U1.

(2) The first user U1 specifies a data content name Tm0 to the key center, presents a user data I1 and a public-key Kb1 of the first user, and requests the distribution of a secret-key Ks1 for decryption and a secret-key Ks2 for re-encryption.

Here, the fee to use the data content M0 is charged.

As the user data, a user ID, a user E-mail address or a secret-key generated at the request of secret-key of the user can be used. Further, random number prepared by the data center as the one specific for the user can be used.

Also, it may be designed in such manner that the data management center combines the first user information (having data amount of several tens of bytes in general) with a first user public-key Kb1 (having data amount of about 1000 bits) and obtains a first user data I1 (having data amount of one thousand and several hundreds of bits), and that MD5 hash value of 16 bytes, obtained by turning the first user data I1 to hash value by MD5 hash algorithm, can be used as the user data.

(3) The key center generates the secret-keys Ks1 and Ks2 and stores them together with a data content name Tm0, the first user data I1 and the first user public-key Kb1, and the secret-keys Ks1 and Ks2 are encrypted using the first user public-key Kb1:

$$Cks1kb1 = E(Ks1, Kb1)$$

$$Cks2kb1 = E(Ks2, Kb1)$$

and the encrypted secret-keys Cks1kb1 and Cks2kb1 are distributed to the first user.

(4) The first user U1 decrypts the secret-keys Cks1kb1 and Cks2kb1 thus distributed using the first user private-key Kv1:

$$Ks1 = D(Cks1kb1, Kv1)$$

$$Ks2 = D(Cks2kb1, Kv1).$$

The decrypted secret-keys Ks1 and Ks2 are stored in the device. The user is not the owner of the secret-keys Ks1 and ks2, but the key center or the data center is the owner. Because there may be possibility of improper use of the secret-keys if the management of the secret-keys is made by the user, the secret-keys Ks1 and Ks2 are automatically stored in IC card, PCMCIA card, insert board or software which are not under user's control.

The secret-keys Ks1 and Ks2 can be generated using the first user data I1. If the data content name and the first user data I1 are available, Ks1 can be generated again. Therefore, it will suffice that the data content name Tm0, the first user data I1 and the first user public-key Kb1 are stored.

The secret-key may be selected each time from library of the key center instead of generating them.

Japanese Patent Laid-Open 271865/1995, as filed by the present inventor, describes a method to divide a copyright management program and to distribute respectively together with data content and key attached thereto.

This method can be applied to the secret-keys themselves, and the secret-key Ks1 can be divided to partial

secret-keys Ks11 and Ks12 as:

$$Ks11 + Ks12 = Ks1$$

and the secret-key Ks2 can be divided to secret-keys Ks21 and Ks22 as:

$$Ks21 + Ks22 = Ks2.$$

The partial secret-keys Ks11 and Ks21 are distributed as partial secret-keys, and the remaining partial secret-keys Ks12 and Ks22 are attached to the data content and distributed. Then, the first user cannot engage any more in the management of the secret-keys Ks1 and Ks2.

(5) The first user U1 presents the first user data I1, specifies the data content name Tm0, and requests the distribution of the data content M0 to the data center.

(6) The data center transfers the first user data I1 and the data content name Tm0 presented by the first user to the key center and asks to transfer the secret-keys Ks1 and Ks2.

(7) The key center transfers the secret-keys Ks1 and Ks2 to the data center.

(8) The data center encrypts the first user data I1 using the public-key Kb0 of the data center:

$$Ci1kb0 = E (I1, Kb0)$$

to an encrypted first user data Ci1kb0. The encrypted first user data Ci1kb0 is entered as an electronic watermark Wci1kb0 to the data content M0, which is requested by the first user U1, and is edited to a data content M1 with electronic watermark:

$$M1 = M0 + Wci1kb0,$$

and this is further encrypted using the secret-key Ks1:

$$Cm1ks1 = E (M1, Ks1).$$

Then, encrypted electronic watermarked data content Cm1ks1 is distributed to the first user U1 by data communication or data broadcasting or by recording on a medium.

The scenario of editing process of the data content M1 (information relating to electronic watermark such as the first user data) is stored to be used for verification.

As a simplified procedure, the first user data I1 may be entered as an electronic watermark Wi1 instead of the encrypted first user data Cilkb0 for the electronic watermark.

(9) The first user U1 decrypts the encrypted electronic watermarked data content Cm1ks1 using the secret-key Ks1 for decryption:

$$M1 = D (Cm1ks1, Ks1)$$

and uses it.

In this case, the secret-key Ks1 is abandoned by the procedure such as overwriting of the secret-key Ks2 on the secret-key Ks1.

(10) When the data content M1 is stored in the storage unit, the data content M1 is re-encrypted using the secret-key Ks2 for re-encryption:

$$Cm1ks2 = E (M1, Ks2)$$

and it is stored as a re-encrypted data content Cm1ks2.

(11) When the first user re-uses the re-encrypted data content Cm1ks2, the first user U1 reads the re-encrypted

data content Cm1ks2 stored in the storage unit on memory, and decrypts it using the secret-key Ks2 and uses it. When the first user stores the data content M1 again, the data content M1 is re-encrypted using the secret-key Ks2 for re-encryption, and the re-encrypted data content Cm1ks2 is stored in the storage unit.

(12) In case the first user transfers the data content M1 to a second user U2, the first user U1 encrypts a second user data I2 using a public-key Kb0 of the data center:

$$Ci2kb0 = E (I2, Kb0),$$

then, enters the encrypted second user data Ci2kb0 as electronic watermark Wci2kb0 in the data content M1 requested by the second user U2, and edits to a data content M2 with electronic watermark:

$$M2 = M1 + Wci2kb0 = (M0 + Wci1kb0) + Wci2kb0.$$

As a simplified procedure, the second user data I2 may be entered as electronic watermark Wi2 instead of the encrypted second user data Ci2kb0.

(13) After the data content M1 with electronic watermark is edited to the data content M2 with electronic watermark, the first user U1 transfers the scenario of editing process of the edited data content M2 (information relating to electronic watermark such as the second user data) to the key center and registers it. As a result, the second user can use the data content.

(14) The key center stores the scenario of editing process registered by the first user, and generates a secret-key Ks3. Then, it is encrypted using the public-key Kb1 of the first user:

$$Cks3kb1 = E (Ks3, Kb1)$$

and the encrypted secret-key Cks3kb1 is distributed to the first user.

(15) The first user U1 decrypts the distributed encrypted secret-key Cks3kb1 using the private-key Kv1 of the first user:

$$Ks3 = D (Cks3kb1, Kv1).$$

(16) Further, data content M2 with electronic watermark is encrypted using the decrypted secret-key Ks3:

$$Cm2ks3 = E (M2, Ks3)$$

and encrypted electronic watermarked data content Cm2ks3 is obtained.

(17) The first user U1 transfers the encrypted electronic watermarked data content Cm2ks3 to the second user U2 by data communication or by copying it on a medium.

(18) The second user U2 stores the transferred encrypted electronic watermarked data content Cm2ks3 in the storage unit.

The second user U2 specifies the data content name Tm0 to the key center, presents the public-key Kb2 of the second user, and requests the distribution of the secret-key Ks3 for decryption and a secret-key Ks4 for re-encryption. (19) The key center confirms according to the stored scenario that the second user U2 is a valid user and generates the secret-key Ks4 and stores it. Then, the secret-key Ks4 and the stored secret-key Ks3 are encrypted using the public-key Kb2 of the second user:

$$Cks3kb2 = E (Ks3, Kb2)$$

$$Cks4kb2 = E (Ks4, Kb2)$$

and the encrypted secret-keys Cks3kb2 and Cks4kb2 are distributed to the second user.

(20) The second user U2 decrypts the encrypted secret-keys Cks3kb2 and Cks4kb2 using the private-key Kv2 of the second user:

$$Ks3 = D (Cks3kb2, Kv2)$$

$$Ks4 = D (Cks4kb2, Kv2)$$

and the decrypted secret-keys Ks3 and Ks4 are stored in IC card, PCMCIA card, insert board or software.

The secret-keys Ks3 and Ks4 at the second user are handled in the same manner as the secret-keys Ks1 and Ks2 at the first user.

(21) The second user U2 reads the encrypted electronic watermarked data content Cm2ks3 stored in the storage unit, on memory, and decrypts it using the stored secret-key Ks3:

$$M2 = D (Cm2ks3, Ks3)$$

and uses it.

Here, the secret-key Ks3 is abandoned by the procedure such as overwriting of the secret-key Ks4 on the secret-key Ks3.

(22) When the data content M2 is stored again in the storage unit, the data content M2 is re-encrypted using the secret-key Ks4 for re-encryption and is stored as a re-encrypted data content Cm2ks4.

(23) In case the second user U2 re-uses the re-encrypted data content Cm2ks4, the re-encrypted data content Cm2ks4 stored in the storage unit is read on memory, and it is decrypted using the secret-key Ks4 and is used.

(24) Further, when the second user stores the data content M2 again, the data content M2 is re-encrypted using the secret-key Ks4 for re-encryption, and the re-encrypted data content Cm2ks4 is stored in the storage unit.

Then, the same procedure is repeated.

The embodiment as described above is arranged under the assumption that the distributed data content is utilized at real time, while it may be designed in such manner that the data content obtained in advance and stored by the user is decrypted later and is used.

In such case, the first user is at the position of the second user in the above embodiment, and similar operation is performed.

As it is evident from the above description, the first user data is entered as electronic watermark in the data content obtained by the first user by the data center.

Therefore, if it is copied and transferred without taking normal procedure, the data center verifies the electronic watermark entered therein, and it is detected that the first user has copied and transferred it without taking normal procedure.

When it is copied and transferred by normal procedure, electronic watermark of each user is entered on the data content, and this clears the route of copying and transfer. When copying and transfer are repeated, noise in the data content increases by the entered electronic watermark, and this makes it possible to limit copying and transfer usage which may increase the risk of illegitimate utilization.

Because a key used for encrypting the data content is stored at the key center, the key center can be utilized when a key escrow system or a key recovery system is used in practical application.

Further, the secret-key can be used as user data, and the secret-key is encrypted using the public-key of the data center and this is entered as electronic watermark. By decrypting this using the private-key of the data center when necessary and by confirming the secret-key, it is possible to achieve a key escrow system or a key recovery system in simple manner but with high security.

[Embodiment 3]

Description will be given on a third embodiment of the invention referring to Fig. 3.

(1) Unlike the first and the second embodiments, the data center and the key center in this embodiment are arranged in such manner that they are a single data management center when seen from the user.

The data management center stores the data content M0 of IP (information provider) in database in advance

or the data content M0 is transferred from IP each time at the request of the first user U1.

(2) The first user U1 specifies a data content name Tm0 to the data management center, presents a user data I1 and a public-key Kb1 of the first user, and requests the distribution of the data content M0 and secret-keys Ks1 and Ks2.

As the user data, a user ID, a user E-mail address or a secret-key generated at the user's request for secret-key can be used. Further, random number prepared by the data center as the one specific for the user can be used.

Also, it may be designed in such manner that the data management center combines the first user information (having data amount of several tens of bytes in general) with a first user public-key Kb1 (having data amount of about 1000 bits) and obtains a first user data I1 (having data amount of one thousand and several hundreds of bits), and that MD5 hash value of 16 bytes, obtained by turning the first user data I1 to hash value by MD5 hash algorithm, can be used as the user data.

(3) The data management center generates the secret-keys Ks1 and Ks2 and encrypts the first user data I1 using the public-key Kb0 of the data center:

$$Ci1kb0 = E (I1, Kb0)$$

to the encrypted first user data Ci1kb0. The encrypted first user data Ci1kb0 is entered in the data content M0 requested by the first user U1 as an electronic watermark Wci1kb0:

$$M1 = M0 + Wci1kb0.$$

Then, a data content M1 with electronic watermark is edited. The data content M1 with electronic watermark is encrypted using the secret-key Ks1:

$$Cm1ks1 = E (M1, Ks1)$$

to encrypted electronic watermarked data content Cm1ks1.

(4) The data management center stores the generated secret-keys Ks1 and Ks2 together with the data content name Tm0, the first user data I1 and the first user public-key Kb1 and encrypts the secret-keys Ks1 and Ks2 using the public-key Kb1 of the first user:

$$Cks1kb1 = E (Ks1, Kb1)$$

$$Cks2kb1 = E (Ks2, Kb1).$$

Then, the two encrypted secret-keys and the encrypted electronic watermarked data content Cm1ks1 are distributed to the first user U1 by data communication or data broadcasting or by recording it on a medium.

The scenario of the editing process of the data content M1 (information relating to electronic watermark such as the first user data) is stored to be used for verification.

As a simplified procedure, the first user data I1 may be entered as electronic watermark Wi1 instead of the encrypted first user data Ci1kb0.

(5) The first user U1 decrypts the encrypted secret-keys Cks1kb1 and Cks2kb1 thus distributed using the first user private-key Kv1:

$$Ks1 = D (Cks1kb1, Kv1)$$

$$Ks2 = D (Cks2kb1, Kv1)$$

and the decrypted secret-keys Ks1 and Ks2 are stored in the device. The user is not the owner of the secret-keys Ks1 and ks2, but the key center or the data center is the owner. Because there may be possibility of improper use of the secret-keys if the management of the secret-keys is made by the user, the secret-keys Ks1 and Ks2 are automatically stored in IC card, PCMCIA card, insert board or software which are not under user's control.

Here, the fee to use the data content M0 is charged.

The secret-keys Ks1 and Ks2 can be generated using the first user data I1. If the data content name and the

first user data I1 are available, Ks1 can be generated again. Therefore, it will suffice that the data content name Tm0 and the first user data I1 are stored.

The secret-key may be selected each time from library of the key center instead of generating them.

Japanese Patent Laid-Open 271865/1995, as filed by the present inventor, describes a method to divide a copyright management program and to distribute respectively together with data content and key attached thereto.

This method can be applied to the secret-keys themselves, and the secret-key Ks1 can be divided to partial secret-keys Ks11 and Ks12 as:

$$Ks11 + Ks12 = Ks1$$

and the secret-key Ks2 can be devided to partial secret-keys Ks21 and Ks22 as:

$$Ks21 + Ks22 = Ks2.$$

The partial secret-keys Ks11 and Ks21 are distributed as partial secret-keys, and the remaining partial secret-keys Ks12 and Ks22 are attached to the data content and distributed. Then, the first user cannot engage any more in the management of the secret-keys Ks1 and Ks2.

(6) The first user U1 decrypts the encrypted electronic watermarked data content Cm1ks1 using the secret-key Ks1 for decryption:

$$M1 = D\ (Cm1ks1,\ Ks1)$$

and uses it.

In this case, the secret-key Ks1 is abandoned by the procedure such as overwriting of the secret-key Ks2 on the secret-key Ks1.

(7) When the data content M1 is stored in the storage unit, the data content M1 is re-encrypted using the secret-key Ks2 for re-encryption:

$$Cm1ks2 = E\ (M1,\ Ks2)$$

and it is stored as a re-encrypted data content Cm1ks2.

(8) When the first user re-uses the re-encrypted data content Cm1ks2, the first user U1 reads the re-encrypted data content Cm1ks2 stored in the storage unit on memory, and decrypts it using the secret-key Ks2 and uses it. When the first user stores the data content M1 again, the data content M1 is re-encrypted using the secret-key Ks2 for re-encryption, and the re-encrypted data content Cm1ks2 is stored in the storage unit.

(9) In case the first user transfers the data content M1 to a second user U2, the first user U1 encrypts a second user data I2 using a public-key Kb0 of the data center:

$$Ci2kb0 = E\ (I2,\ Kb0).$$

Then, the encrypted second user data Ci2kb0 is entered as electronic watermark Wci2kb0 in the data content M1 requested by the second user U2 and is edited to a data content M2 with electronic watermark:

$$M2 = M1 + Wci2kb0 = (M0 + Wci1kb0) + Wci2kb0.$$

As a simplified procedure, the second user data I2 may be entered as electronic watermark Wi2 instead of the encrypted second user data Ci2kb0.

(10) After editing to the data content M2 with electronic watermark, the first user U1 transfers the scenario of the editing process of the edited data content M2 (information relating to electronic watermark such as the second user data) to the data management center and registers it. As a result it is possible to utilize the data content by the second user.

(11) Further, the first user U1 encrypts the data content M2 with electronic watermark using the secret-key Ks2:

$$Cm2ks2 = E(M2, Ks2)$$

and encrypted electronic watermarked data content Cm2ks2 is obtained.

(12) The first user U1 transfers the encrypted electronic watermarked data content Cm2ks2 to the second user U2 by data communication or by copying it on a medium.

(13) The second user U2 stores the transferred encrypted electronic watermarked data content Cm2ks2 in the storage unit.

The second user U2 specifies the data content name Tm0 to the data management center, presents the public-key Kb2 of the second user, and requests the distribution of the secret-key Ks2 for decryption and the secret-key Ks3 for re-encryption.

(14) The data management center confirms according to the stored scenario that the second user U2 is a valid user and generates the secret-key Ks3 and stores it. Then, the stored secret-key Ks2 and the generated secret-key Ks3 are encrypted using the public-key Kb2 of the second user;

$$Cks2kb2 = E(Ks2, Kb2)$$

$$Cks3kb2 = E(Ks3, Kb2).$$

Then, the encrypted secret-keys Cks2kb2 and Cks3kb2 are distributed to the second user.

(15) The second user U2 decrypts the encrypted secret-keys Cks2kb2 and Cks3kb2 using the private-key Kv2 of the second user:

$$Ks2 = D(Cks2kb2, Kv2)$$

$$Ks3 = D(Cks3kb2, Kv2).$$

The decrypted secret-keys Ks2 and Ks3 are stored in IC card, PCMCIA card, insert board or software.

The secret-keys Ks2 and Ks3 at the second user are handled, and decrypted and stored in the same manner as the secret-keys Ks1 and Ks2 at the first user.

(16) The second user U2 reads the encrypted electronic watermarked data content Cm2ks2 stored in the storage unit, on memory, and decrypts it using the stored secret-key Ks2:

$$M2 = D(Cmsks2, Ks2)$$

and uses it.

In this case, the secret-key Ks2 is abandoned by the procedure such as overwriting of the secret-key Ks3 on the secret-key Ks2.

(17) When the data content M2 is stored again in the storage unit, the data content M2 is re-encrypted using the secret-key Ks3 for re-encryption, and it is stored as the re-encrypted data content Cm2ks3.

(18) When the second user U2 re-uses the re-encrypted data content Cm2ks3, the re-encrypted data content Cm2ks3 stored in the storage unit is read on memory, and it is decrypted using the secret-key Ks3 and is used.

(19) Further, when the second user stores the data content M2 again, the data content M2 is re-encrypted using the secret-key Ks3 for re-encryption, and the re-encrypted data content Cm2ks3 is stored in the storage unit.

Then, the same procedure is repeated.

The embodiment as described above is arranged under the assumption that the distributed data content is utilized at real time, while it may be designed in such manner that the data content obtained in advance and stored by the user is decrypted later and is used.

In such case, the first user is at the position of the second user in the above embodiment, and similar operation is performed.

As it is evident from the above description, the first user data is entered as electronic watermark in the data content obtained by the first user by the data center.

Therefore, if it is copied and transferred without taking normal procedure, the data center verifies the electronic watermark entered therein, and it is detected that the first user has copied and transferred it without taking normal procedure.

When it is copied and transferred by normal procedure, electronic watermark of each user is entered in the data content, and this clears the route of copying and transfer. When copying and transfer are repeated, noise in the data content increases by the entered electronic watermark, and this makes it possible to limit copying and transfer usage which may increase the risk of illegitimate utilization.

Because a key used for encrypting the data content is stored at the data management center, the data management center can be utilized when a key escrow system or a key recovery system is used in practical application.

[Embodiment 4]

Description will be given now on the fourth embodiment of the invention referring to Fig. 4A and Fig. 4B.

Unlike the first to the third embodiments, which relate to the data management system as a whole, the fourth embodiment is directed to data management operation on the user side. The flow chart shown in Fig. 4A represents an example of the operation performed on a first user side, and the flow chart shown in Fig. 4B represents an example of the operation on a second user side.

In this embodiment, the data management program is arranged as an object program, and the user data and the secret-key are stored as instance variables in the slot of the object.

(1) The first user U1 obtains an encrypted data content Cm0ks1 which is obtained through encrypting the data content M0 using a first secret-key Ks1. The encrypted data content can be obtained via a network, by data broadcasting, or via a recording medium.

(2) When the encrypted data content Cm0ks1 is obtained, the first user U1 obtains the data management program object where first secret-key Ks1 is stored in the slot as instance variable, from the data management center. The data management program object may be provided via the network, but it is desirable to supply it by storing in an IC card or the like for security purpose.

(3) The first user data I1 is stored as instance variable in the slot of the data management program object.

(4) It is confirmed that the first user data I1 has been stored in the data management program object.

If not stored, the procedure of (3) above to store the first user data I1 to the data management program object is repeated.

(5) A pattern of electronic watermark W1 is generated based on the first user data I1 by the data management program.

(6) The first user U1 decrypts the encrypted data content Cm0ks1 using the first secret-key Ks1:

$$M0 = D\,(Cm0ks1,\ Ks1).$$

The decrypted data content M0 is edited by promptly entering the electronic watermark W1, and the data content M0 is edited to a data content M1.

(7) A second secret-key is generated by the data management program.

(8) By overwriting the generated second secret-key on the first secret-key, the first secret-key Ks1 is abandoned, and the second secret-key Ks2 is stored.

(9) After the above procedure has been completed, the data content M1 is utilized.

The data content to be utilized is not the data content M0 obtained from the data management center, but it is the data content M1 where the user data I1 of the first user U1 is entered as electronic watermark. However, the electronic watermark gives no change to external appearance, and it can be used without any trouble.

(10) When the data content M1 used by the first user U1 is to be stored in the storage unit, the data content M1 is first encrypted using the second secret-key Ks2 by the data management program:

$$Cm1ks2 = E(M1, Ks2).$$

(11) Then, it is confirmed whether the data content M1 to be stored has been turned to the encrypted data content Cm1ks2 or not. In case it is not encrypted, the data content is not stored, and it goes back to the step in (9) above.

(12) When it is confirmed that the data content to be stored is the encrypted data content Cm1ks2, the encrypted data content Cm1ks2 is stored in the storage unit.

(13) In case the first user U1 re-uses the encrypted data content Cm1ks2 without copying and transferring to the second user U2,

(14) the encrypted data content Cm1ks2 stored in the storage unit is read,

(15) the encrypted data content Cm1ks2 is decrypted using the second secret-key Ks2 by the data management program:

$$M1 = D(Cm1ks2, Ks2),$$

and

(16) the decrypted data content M1 is used.

(17) When the first user U1 stores the re-used data content M1 to the storage unit, the data content M1 is first re-encrypted using the second secret-key Ks2 by the data management program and is stored.

(18) In case the first user U1 copies and transfers the encrypted data content Cm1ks2 to the second user U2, the encrypted data content Cm1ks2 is transferred by copying it on a recording medium or via the network.

(19) The second user U2 obtains the encrypted data content Cm1ks2 via the network or via the recording medium.

(20) When the encrypted data content Cm1ks2 is obtained, the second user U2 obtains the data management program object where the second secret-key Ks2 is stored in the slot as instance variable, from the data management center. The data management program object may be provided via the network but it is desirable to supply it by storing in an IC card or the like for security purpose.

(21) The second user data I2 is stored as instance variable in the slot of the data management program object.

(22) It is confirmed that the second user data I2 has been stored in the data management program object.
If not stored, the procedure in (21) above to store the second user data I2 to the data management program object is repeated.

(23) By the data management program, a pattern of electronic watermark W2 based on the second user data I2 is generated.

(24) The second user U2 decrypts the encrypted data content Cmlks2 using the second secret-key Ks2:

$$M1 = D(Cm1ks2, Ks2).$$

The decrypted data content M1 is edited by promptly entering the electronic watermark W2, and the data content M1 is edited to a data content M2.

(25) A third secret-key is generated by the data management program.

(26) By overwriting the generated third secret-key on the second secret-key, the second secret-key Ks2 is abandoned, and the third secret-key Ks3 is stored.

(27) After the above procedure has been completed, the data content M2 is utilized.

The data content to be utilized is not the data content M0 obtained from the data management center, but it is the data content M2 where the data I2 of the second user U2 is entered as electronic watermark. However, the electronic watermark gives no change to external appearance, and it can be used without any trouble.

By overwriting the electronic watermark W2 on the electronic watermark W1, such as only W2 is entered in the data content M2, it is possible to design in such manner that a single electronic watermark is entered at all times and it is only the electronic watermark of the final user data. Or else, such as the electronic watermark W2 may be written at the same time without overwriting on the electronic watermark W1 in the data content M2, it is also possible that the electronic watermarks entered increase and these are the electronic watermarks of all of the user data.

(28) When the data content M2 used by the second user U2 is to be stored in the storage unit, the data content M2 is first encrypted using the third secret-key Ks3 by the data management program:

$$Cm2ks3 = E(M2, Ks3).$$

(29) Then, it is confirmed whether the data content M2 to be stored has been turned to the encrypted data content Cm2ks3 or not. If it is not encrypted, the data content is not stored, and it goes back to the step of (27).

(30) When it is confirmed that the data content to be stored is the encrypted data content Cm2ks3, the encrypted data content Cm2ks3 is stored in the storage unit.

(31) In case the second user U2 re-uses the encrypted data content Cm2ks3 without copying and transferring it to the third user U3,

(32) the encrypted data content Cm2ks3 stored in the storage unit is read,

(33) the encrypted data content Cm2ks3 is decrypted using the third secret-key Ks3 by the data management program:

$$M2 = D(Cm2ks3, Ks3),$$

and

(34) the decrypted data content M2 is utilized.

(35) When the second user U2 stores the re-used data content M2 in the storage unit, the data content M2 is first re-encrypted by the data management program using the third secret-key Ks3 and is stored.

(36) In case the second user U2 copies and transfers the encrypted data content Cm2ks3 to the third user U3, the encrypted data content Cm2ks3 is copied on a recording medium or is provided via the network.

Then, the same procedure is repeated.

The first to the fourth embodiments as described above represent the cases where illegitimate use of the data under control of the data management center is prevented, i.e., a charged key is used for a charged data.

However, in the arrangement as described above, by replacing the data management center with a host of video conference, the first user with a guest of video conference, and the second and the subsequent users with observers of video conference, it is possible in the application to a video conference system to prevent leakage of the content of the conference.

Similarly, in the application to a digital cash system, by replacing the data management center with a client side bank, the first user with a client, and the second user with a shop, it is possible to improve security in the digital cash system.

In the system as described above, each of the users to utilize the system must be registered at the data management center in advance. At the time of registration, data management program is provided to the users.

In the present invention to utilize the data M, the first secret-key Ks1, the second secret-key Ks2 and the data management program are transferred to each user, and each user must store them.

As the place to store them, it is ideal to use an IC card now being propagated, in which an IC element is encapsulated in a card-like container, or in particular, to use a PC card where microprocessor is encapsulated.

Also, it is possible to design in such manner that the data management program serves as an agent on the data management center side so that utilization status, transfer status, etc. of the data content are automatically reported when the user sends a request to use to the data management center.

Claims

1. Data management system, in which users utilize data content of a data center, comprising a data management center comprising a data center and a key center; wherein:

   the data center is enabled:
   to transfer user data presented by a user and data content names to the key center and to receive first and second secret-keys;
   to enter said user data as electronic watermark in a data content and to edit it in form of an edited data content and to encrypt edited data content using said first secret-key to produce encrypted edited data content;
   to transfer encrypted edited data content and said first and second secret-keys to users; and
   to store a scenario of the editing process;
   the key center is enabled:
   to generate first and second secret-keys, to store data content names, user data, first and second secret keys and scenarios of users, to transfer said first and second secret-keys to users and to the data center together with user data and data content names; and to confirm by a scenario transferred by a user whether the user is an authorized user.

2. Data management system, in which users utilize data content of a data center, comprising a data management center having a data center and a key center; wherein

   the data management center is enabled:
   to generate first and second secret-keys and transfer it to users,
   to store data content names, user data, said first and second secret-keys and
   scenarios of the editing process of an edited data content;
   to enter user data as electronic watermark in data content to obtain edited data content, to encrypt the edited data content with said first secret-key to obtain an encrypted edited data content ;
   to transfer said first and second secret keys to the users; and
   to confirm by a stored scenario that a user is an authorized user

3. Data management system, in which users utilize data content of a data management center, comprising:

   a data management center enabled to distribute a data management program designed as an object program which stores a user data and a secret-key in a slot; wherein:

   a first user obtains an encrypted data content encrypted using a first secret-key;
   when said encrypted data content is obtained, said first user obtains the data management program object stored in said slot with said first secret-key from said data management center, and stores the first user data in the slot of said data management program object;
   when it is confirmed by said data management program that said first user data is already stored in said data management program object, an electronic watermark is generated based on said first user data; said encrypted data content is decrypted using said first secret-key, and the data content thus decrypted is entered promptly said electronic watermark therein to be first edited data content; a second secret-key is generated by said data management program and is stored, and said first secret-key is abandoned at this time;

   said first edited data content is then used;
   when said first edited data content is stored, said first edited data content is encrypted first using said second secret-key to be an encrypted first edited data content;
   when it is confirmed that said first edited data content has been the encrypted first edited data content, said encrypted first edited data content is stored; when said first user re-uses said encrypted first edited data content, said encrypted first edited data content is decrypted using said second secret-key and is used;
   when said first edited data content re-used by said first user is stored, said first edited data content is re-

encrypted using said second secret-key, and said encrypted first edited data content is stored;
when said first user copies and transfers said encrypted first edited data content to a second user, said encrypted first edited data content is copied and transferred; and

the same operation is repeated thereafter.

4. Process for managing data, when users utilize a data content of a data center, wherein a data management center comprises a data center and a key center according to claim 1; comprising the steps of:

specifying a data content name to said key center, presentation of a user data and requesting transfer of a first secret-key and a second secret-key by a first user;
when requested to transfer said first secret-key and said second secret-key, generating said first secret-key and said second secret-key, storing said data content name, first user data, said first secret-key and said second secret-key, and transfer of said first secret-key and said second secret-key to said first user by said key center;
when said first secret-key and said second secret-key are received, storing said first secret-key and said second secret-key thus transferred in a storage unit by said first user;
when said first secret-key and said second secret-key are stored in the storage unit, presentation of said first user data, specifying said data content name, and requesting said data center to transfer the data content by said first user;
when requested to transfer said data content, transfer of said first user data and said data content name presented by said first user to said key center, asking to transfer said first secret-key and said second secret-key by said data center;
when said first user data and said data content name are received, transfer of said first secret-key and said second secret-key to said data center by said key center;
when said first secret-key and said second secret-key are received: entering said first user data as electronic watermark in said data content as requested by said first user and editing it as a first edited data content, encrypting said first edited data content using said first secret-key to obtain an encrypted first edited data content, transfer thereof to said first user and storing a first scenario of editing process of said first edited data content by said data center;
when said encrypted first edited data content is received, decrypting said encrypted first edited data content using said first secret-key and using it, and abandoning said first secret-key at this time by said first user;
when said first edited data content is stored in the storage unit, encrypting said first edited data content using said second secret-key and storing it;
when said encrypted first edited data content is reused, re-decrypting it using said second secret-key and re-using it;
when said first edited data content is stored again, encrypting it again using said second secret-key and storing it;
when said first user transfers said first edited data content to a second user, entering a second user data as electronic watermark in said first edited data content to edit it to a second edited data content, encrypting said second edited data content using said second secret-key to obtain an encrypted second edited data content, transfer thereof to said second user, and transfer of a second scenario of editing process of said second edited data content to said key center and having it registered by said first user;
when said encrypted second edited data content is transferred, specifying said data content name to said key center, presentation of said second user data, and requesting transfer of said second secret-key and a third secret-key by said second user;
when requested to transfer said second secret-key and said third secret-key, confirmation by said second scenario that said second user is a valid user, generation and storing said third secret-key, and transfer of said second secret-key and said third secret-key to said second user by the key center;
when said second secret-key and said third secret-key are transferred, decrypting said encrypted second edited data content using said second secret-key and using it by said second user, and at this time said second secret-key being abandoned;
when said second edited data content is stored, re-encrypting it using said third secret-key and storing it;
when the encrypted second edited data content is re-used, decrypting it using said third secret-key and re-using it;
when said second edited data content is stored again, re-encrypting said second edited data content using said third secret-key and storing it again; and

repeating the same operation/s thereafter.

5. Process for managing data according to claim 1, in which users utilize data content of a data center, wherein a data management center comprises a data center and a key center; comprising the steps:

specifying a data content name to said key center, presentation of user data and requesting transfer of a first secret-key and a second secret-key by a first user;
when requested to transfer said first secret-key and said second secret-key, generation of said first secret-key and said second secret-key, storing said data content name, first user data, said first secret-key and said second secret-key, and transfer of said first secret-key and said second secret-key to said first user by said key center;
when said first secret-key and said second secret-key are transferred, storing said first secret-key and said second secret-key in a storage unit by said first user;
when said first secret-key and said second secret-key are stored in the storage unit, presentation of said first user data, specifiying of said data content name, and requesting said data center to transfer the data content by said first user;
when requested to transfer said data content, transfer of said first user data and said data content name presented by said first user to said key center and asking to transfer said first secret-key and said second secret-key by said data center;
when said first user data and said data content name are transferred, transfer of said first secret-key and said second secret-key to said data center by said key center;
when said first secret-key and said second secret-key are transferred, entering said first user data as electronic watermark into said data content as requested by said first user and editing it to a first edited data content, encrypting said first edited data content using said first secret-key to obtain an encrypted first edited data content, transfer thereof to said first user and storing a first scenario of editing process of said first edited data content by said data center;
when said encrypted first edited data content is transferred, decrypting said encrypted first edited data content using said first secret-key and using it by said first user, and at this time said first secret-key being abandoned;
when said first edited data content is stored in the storage unit, encrypting said first edited data content using said second secret-key and storing it; when said encrypted first edited data content is re-used, decrypting it again using said second secret-key and re-using it;
when said first edited data content is stored again, re-encrypting said first edited data content using said second secret-key and storing it again;
when said first user transfers said first edited data content to a second user, entering a second user data as electronic watermark in said first edited data content to edit it to a second edited data content, encrypting said second edited data content using said second secret-key to obtain an encrypted second edited data content, transfer thereof to said second user, and transfer of a second scenario of editing process of said second edited data content to said key center and having it registered by said first user
when said second scenario is transferred, generation of a third secret-key, storing said second scenario and said third secret-key, and transfer of said third secret-key to said first user by said key center;
when said third secret-key is transferred, encrypting said second edited data content using said third secret-key, and transfer of the encrypted second edited data content to said second user by said first user;
when said encrypted second edited data content is transferred, specifying said data content name to said key center, presentation of the second user data and requesting transfer of said third secret-key and a fourth secret-key by said second user;
when requested to transfer said third secret-key and said fourth secret-key, confirmation by said second scenario that said second user is a valid user, generation and storing said fourth secret-key, and transfer of said third secret-key and said fourth secret-key to said second user by said key center;
when said third secret-key and said fourth secret-key are transferred, decrypting said encrypted second edited data content using said third secret-key and using it by said second user, and at this time said third secret-key being abandoned;
when said second edited data content is stored, re-encrypting said second edited data content using said fourth secret-key and storing it;
when said encrypted second edited data content is re-used, decrypting it using said fourth secret-key and re-using it;
when said second edited data content is stored again, re-encrypting said second edited data content using said fourth secret-key and storing it again; and

repeating the same operation/s thereafter.

6. Process for managing data according to claim 2, in which users utilize a data content of a data center, wherein a data management center comprises a data center and a key center; comprising the steps:

specifying of a data content name to said data management center, presentation of a user data, and request of transfer of a first secret-key, a second secret-key and data content by a first user;
when requested to transfer said first secret-key, said second secret-key and said data content, generation of said first secret-key and said second secret-key, storing said data content name, first user data, said first secret-key and said second secret-key, entering said first user data as electronic watermark in said data content to edit it as a first edited data content, encrypting said first edited data content using said first secret-key to obtain an encrypted first edited data content, transfer of said encrypted first edited data content to said first user, and storing a first scenario of editing process of said first edited data content by said data management center;
when said first secret-key, said second secret-key and said encrypted first edited data content are received, storing said first secret-key and said second secret-key thus transferred in a storage unit, and decrypting said encrypted first edited data content using said first secret-key and using it by said first user, and at this time said first secret-key being abandoned;
when said first edited data content is stored in the storage unit, encrypting said first edited data content using said second secret-key and storing it;
when said encrypted first edited data content is re-used, decrypting it again using said second secret-key and re-using it;
when said first edited data content is stored again in the storage unit, re-encrypting said first edited data content using said second secret-key and storing it again;
when said first user transfers said first edited data content to a second user, entering his second user data as electronic watermark in said first edited data content to edit it to a second edited data content, encrypting said second edited data content using said second secret-key to obtain an encrypted second edited data content, transfer thereof to said second user, and transfer of a second scenario of editing process of said second edited data content to said data management center and having it registered by said first user;
when said encrypted second edited data content is transferred, specifying said data content name to said data management center, presentation of said second user data, request of transfer of said second secret-key and a third secret-key by said second user;
when requested to transfer said second secret-key and said third secret-key, confirmation by said second scenario that said second user is a valid user, generation and storing of said third secret-key, and transfer of said second secret-key and said third secret-key to said second user by said data management center;
when said second secret-key and said third secret-key are received, decrypting said encrypted second edited data content using said second secret-key and using it by said second user, and at this time said second secret-key being abandoned;
when said second edited data content is stored, re-encrypting it using said third secret-key and storing it;
when said second edited data content is reused, decrypting it using said third secret-key and re-using it;
when said second edited data content is stored again, re-encrypting said second edited data content using said third secret-key and storing it again; and

repeating the same operation/s thereafter.

7. Process for managing data in which users utilize data of a data management center according to claim 3, comprising the steps of:

having a data management program designed as an object program which stores user data and a secret-key in a slot;

obtaining an encrypted data content encrypted using a first secret-key by a first user;
when said encrypted data content is obtained, obtaining the data management program object stored in said slot with said first secret-key from said data management center, and storing the first user data in the slot of said data management program object by said first user;
when it is confirmed by said data management program that said first user data is already stored in said data management program object, generation of an electronic watermark on basis of said first user data;

decrypting said encrypted data content using said first secret-key, and promptly entering said electronic watermark into the data content thus decrypted and obtaining a first edited data content;

generation and storing a second secret-key by said data management program, and at this time said first secret-key being abandoned;

using said first edited data content then;
when said first edited data content is stored, encrypting said first edited data content first using said second secret-key to an encrypted first edited data content;
when it is confirmed that said first edited data content has been the encrypted first edited data content, storing said encrypted first edited data content;
when said first user re-uses said encrypted first edited data content, decrypting said encrypted first edited data content using said second secret-key and using it;
when said first edited data content re-used by said first user is stored, re-encrypting said first edited data content using said second secret-key, and storing said encrypted first edited data content;
when said first user copies and transfers said encrypted first edited data content to a second user, copying and transfer of said encrypted first edited data content; and

repeating of the same operation/s thereafter.

Fig. 1

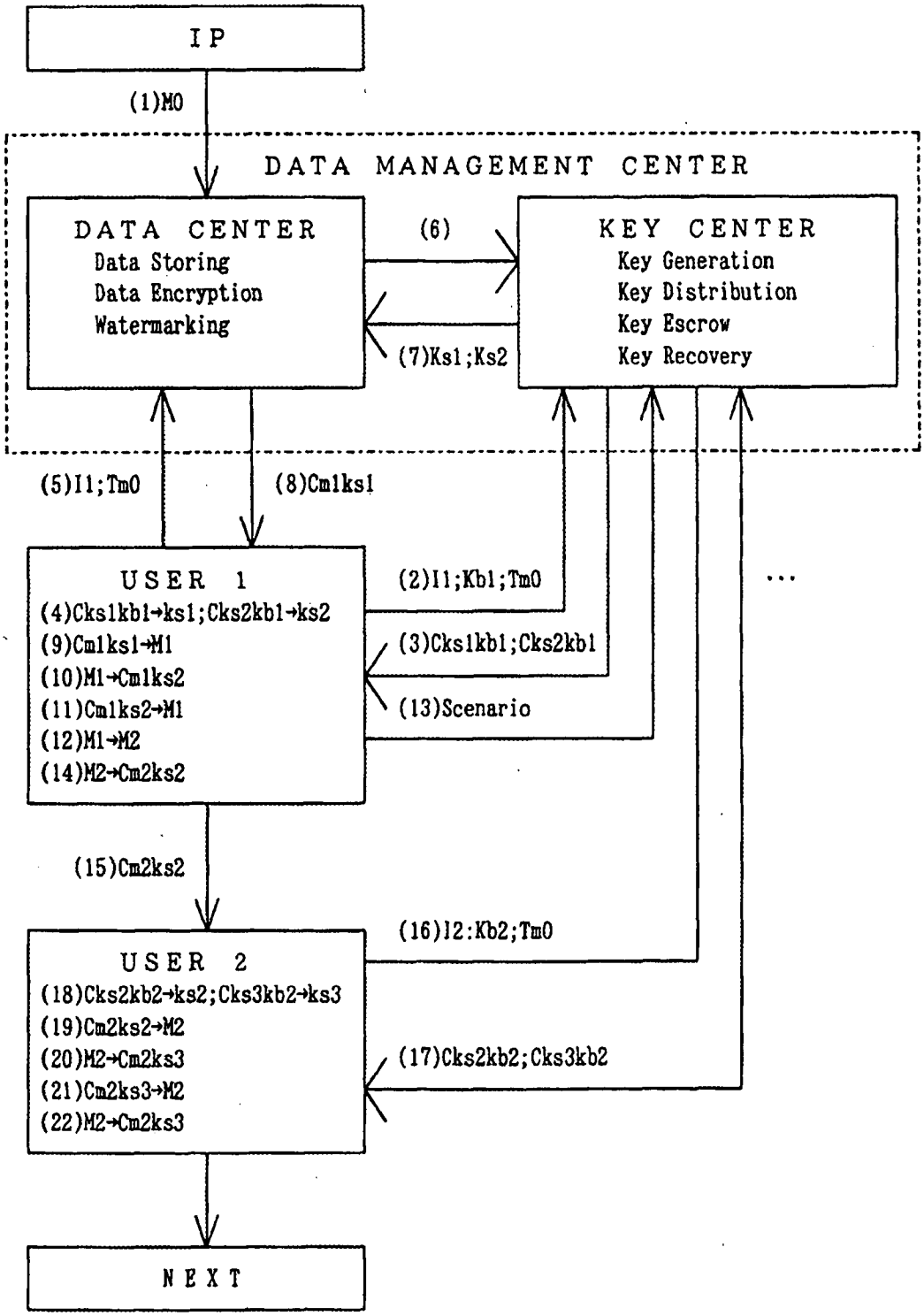


Fig. 2

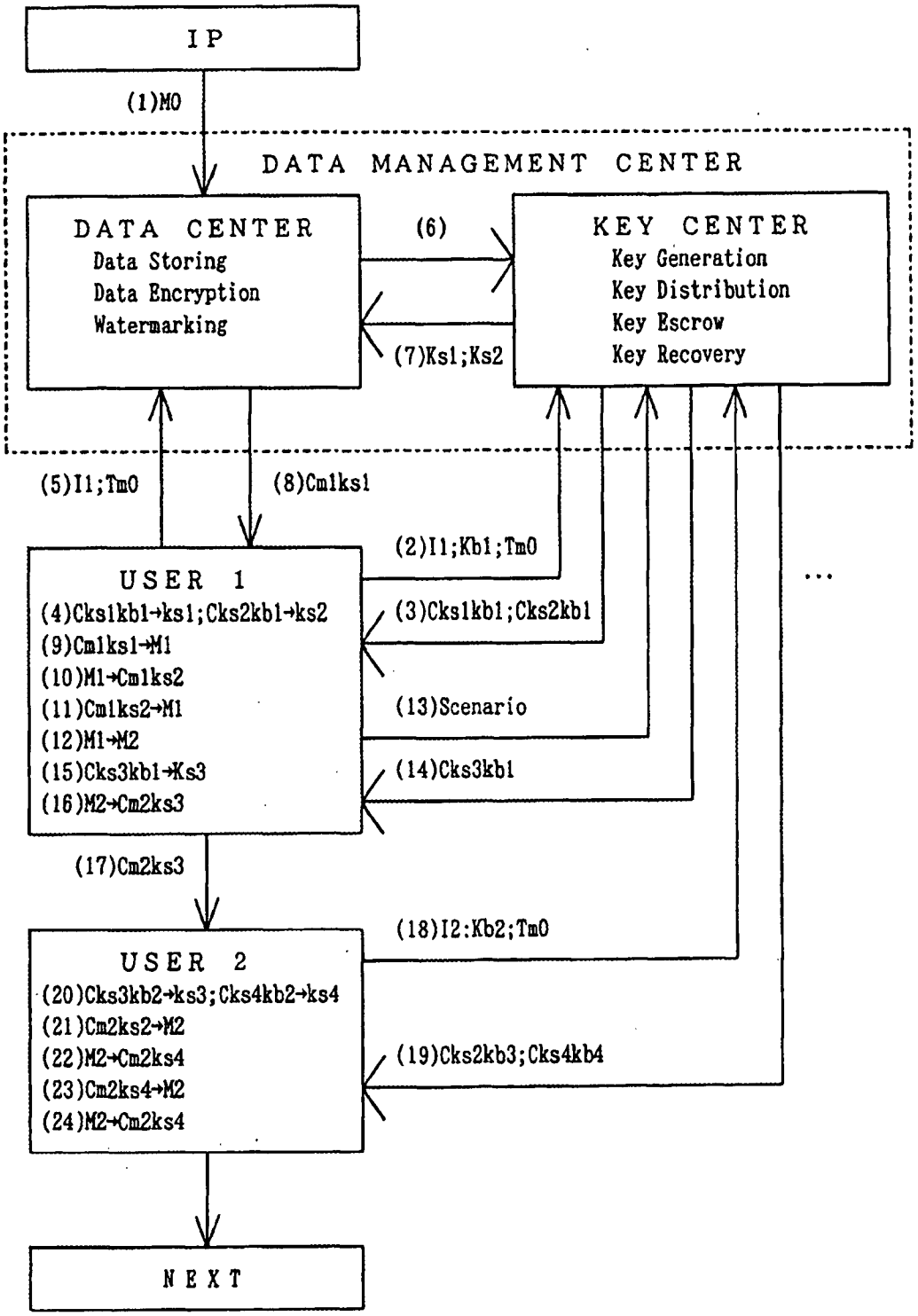


Fig. 3

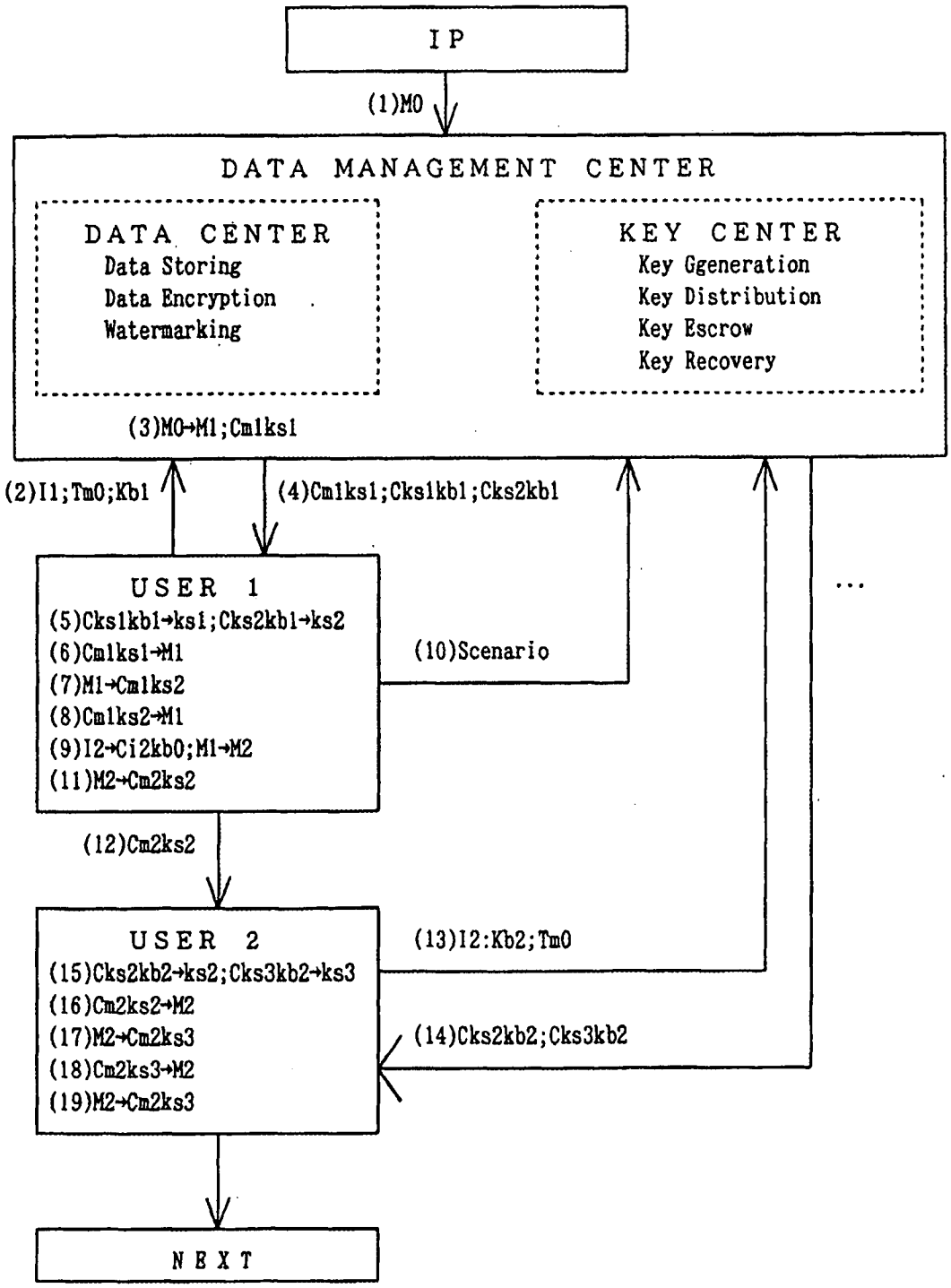


Fig. 4A

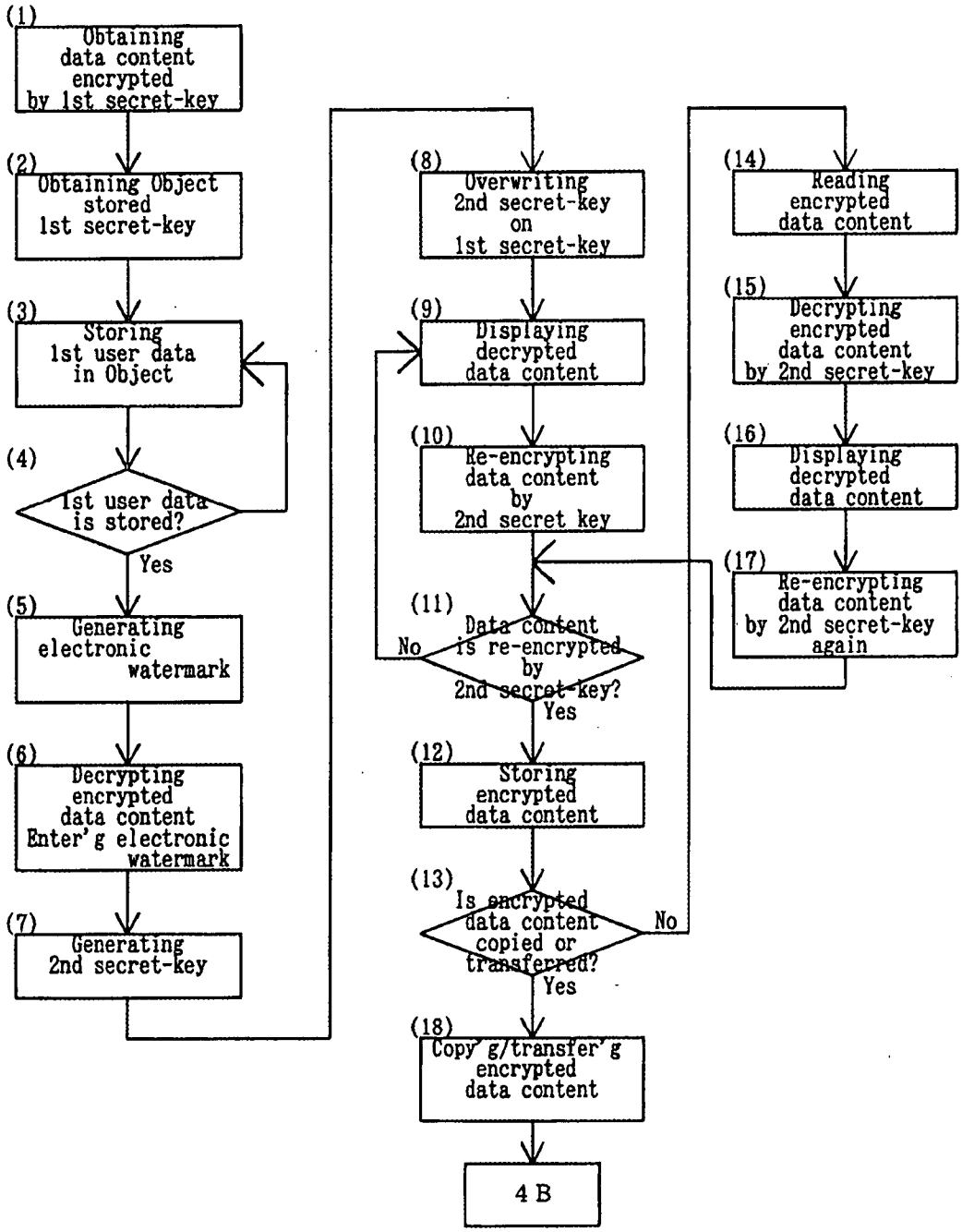


Fig. 4B